

[Redacted]
UNCLASSIFIED//~~FOUO~~**FEDERAL BUREAU OF INVESTIGATION****Complaint Form****Title:** (U) PAL2017 [Redacted] **E-Tip:** Extortion **Date:** 06/29/2017b3
b6
b7C
b7E**Approved By:** [Redacted]**Drafted By:** [Redacted]**Case ID #:** [Redacted] (U//~~FOUO~~) CYBER-FINANCIALLY MOTIVATED
CRIMINAL; [Redacted] BEGIN 3/6
/2014

b7E

[Large redacted area]

Complaint Synopsis: (U) Report to the FBI Public Access Line (PAL)
Unit via www.ic3.gov by [Redacted] of extortion predicated via email
from Lizard Squad in Lenexa, KS. (KC)b6
b7C**Received On:** 05/01/2017**Receipt Method:** Other**Incident Type:** Criminal Activity**Drafted By:** [Redacted]**Complaint Details:**b6
b7C[Redacted]
[Redacted] business

name Small Business Bank, address 13423 W 92nd St, Lenexa, KS66215,

UNCLASSIFIED//~~FOUO~~

[REDACTED]
UNCLASSIFIED//~~FOUO~~

Title: (U) PAL2017 [REDACTED] E-Tip: Extortion
Re: [REDACTED] 06/29/2017

submitted an online tip via www.ic3.gov, which was forwarded to the FBI Public Access Line (PAL) Unit, of extortion predicated via email from Lizard Squad.

Date Submitted: [REDACTED]

Transaction Number: [REDACTED]

b6
b7C
b7E

Submitted Text:

IC3 Complaint ID: [REDACTED]

Date: [REDACTED]

Filed from: [REDACTED]

Victim Information

Name: [REDACTED]

Business Name: Small Business Bank

Age: [REDACTED]

Address: 13423 W 92nd St

Address (continued):

Suite/Apt./Mail Stop:

b6
b7C

City: Lenexa

County: Johnson

State: Kansas

Country: United States of America

Zip Code/Route: 66215

Phone Number: [REDACTED]

E-mail Address: [REDACTED]

Business IT POC: [REDACTED]

Other Business POC:

Financial Transactions

Transaction Type: Other

Transaction Amount: \$8.00

Transaction Date: 05/04/2017

Victim Bank Name: Small Business Bank

Victim Bank Address: 13423 W 92nd St

Victim Bank Address (continued):

Victim Bank Suite/Mail Stop:

UNCLASSIFIED//~~FOUO~~

[REDACTED]
UNCLASSIFIED//~~FOUO~~

Title: (U) PAL2017 [REDACTED] E-Tip: Extortion
Re: [REDACTED] 06/29/2017

Victim Bank City: Lenexa

Victim Bank State: Kansas

Victim Bank Country: United States of America

Victim Bank Zip Code/Route: 66215

Victim Name on Account: NA

Victim Account Number:

Recipient Bank Name: Unknown - Bitcoin address

[REDACTED] Recipient Bank Address:

Recipient Bank Address (continued):

Recipient Bank Suite/Mail Stop:

Recipient Bank City:

Recipient Bank State:

Recipient Bank Country:

Recipient Bank Zip Code/Route:

Recipient Name on Account:

Recipient Bank Routing Number:

Recipient Account Number:

Recipient Bank SWIFT Code:

b6
b7C
b7E

Description of Incident: Please see the e-mail chain below for details. The Customer Service e-mail address received a Lizard Squad threat on Saturday, 29-Apr-17 at 17:12 local time. This was forwarded to the bank's Managed IT Service Provider, Network Technologies, Inc. on Monday, 1-May-17.

From: SmallBusinessBank.com

Sent: Monday, May 01, 2017 8:53 AM

To: [REDACTED]

b6
b7C
b7E

Subject: FW: New SBB Web Contact Form Submission

from: Lizard Squad

I am going to assume this is just a bogus threat, but I am forwarding it to you anyway. Thanks, [REDACTED]

From: Lizard Squad [mailto:[REDACTED]]

Sent: Saturday, April 29, 2017 5:12 PM

To: SmallBusinessBank.com; [REDACTED] <mailto:[REDACTED]

[REDACTED]
UNCLASSIFIED//~~FOUO~~

[REDACTED]

UNCLASSIFIED//~~FOUO~~

Title: (U) PAL2017 [REDACTED] E-Tip: Extortion
Re: [REDACTED] 06/29/2017

Subject: New SBB Web Contact Form Submission
from: Lizard Squad
Name Lizard Squad
Your Email Address [REDACTED] kmailto:
[REDACTED]

Phone Number [REDACTED]

Subject DDoS Attack Imminent - Important information Message PLEASE FORWARD THIS EMAIL TO SOMEONE IN YOUR COMPANY WHO IS ALLOWED TO MAKE IMPORTANT DECISIONS! We are the Lizard Squad and we have chosen your company as target for our next DDoS attack. Please perform a google search for "Lizard Squad DDoS" and "Mirai Botnet" to have a look at some of our previous "work". Your network will be subject to a DDoS attack starting at Thursday the 4th of May. What does this mean? This means that your website and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation amongst your users / customers as well as strongly hurt your google rankings (worst case = your website will get de-indexed). How do I stop this? We are willing to refrain from attacking your servers for a small fee. The current fee is 8 Bitcoins (BTC). The fee will increase by 8 Bitcoins for each day after Thursday that has passed without payment. Please send the bitcoin to the following Bitcoin address: [REDACTED] Once you have paid we will automatically get informed that it was your payment. Please note that you have to make payment before Thursday the 4th of May or the attack WILL start! How do I get Bitcoins? You can easily buy bitcoins via several websites or even offline from a Bitcoin-ATM. We suggest you to start with localbitcoins.com or do a google search. What if I don't pay? If you decide not to pay, we will start the attack at the indicated date and uphold it until you do, there's no counter measure to this, you will only end up wasting more money trying to find a solution. We will completely destroy your reputation amongst google and your customers and make sure your services will remain offline until you pay. This is not a hoax, do not reply to this email, don't try to reason or negotiate, we will not read any replies. Once you have paid we won't start the attack and you will never hear from us again! Please note that Bitcoin is anonymous and no

b6
b7C
b7E

b7E

UNCLASSIFIED//~~FOUO~~

[REDACTED]
UNCLASSIFIED//~~FOUO~~

Title: (U) PAL2017 [REDACTED] E-Tip: Extortion
Re: [REDACTED] 06/29/2017

one will find out that you have complied. >From Page: <https://www.smallbusinessbank.com/about/contact/> Disclaimer The information contained in this communication from the sender is confidential. It is intended solely for use by the recipient and others authorized to receive it. If you are not the recipient, you are hereby notified that any disclosure, copying, distribution or taking action in relation of the contents of this information is strictly prohibited and may be unlawful. This email has been scanned for viruses and malware, and may have been automatically archived by Mimecast Ltd, an innovator in Software as a Service (SaaS) for business. Providing a safer and more useful place for your human generated data. Specializing in; Security, archiving and compliance. To find out more visit the Mimecast website.

Used in this incident:

Other: E-mail threat

Subject Information

Business Name: The Lizard Squad Name:

Address:

Address (continued):

Suite/Apt./Mail Stop:

City: Olathe

State: Kansas

Country: United States of America

Zip Code/Route: 66062

Phone Number: [REDACTED]

E-mail Address: [REDACTED]

Website:

IP Address:

Other Information

If an email was used in this incident, please provide a copy of the entire email including full email headers. [No response provided]

If you have reported this incident to other law enforcement or a government agency, please provide the name, phone number, email, date reported, report number, etc. No other law enforcement contacted at this time.

b6
b7C
b7E

UNCLASSIFIED//~~FOUO~~

[REDACTED]

UNCLASSIFIED//~~FOUO~~

Title: (U) PAL2017 [REDACTED] E-Tip: Extortion
Re: [REDACTED] 06/29/2017

Are there any other witnesses or victims to this incident? [No response provided]

Complainant Info

Complainant Name: [REDACTED]

b6
b7C

Complainant Business Name: Network Technologies, Inc.

Complainant Phone Number: [REDACTED]

Complainant Email Address: [REDACTED]

Tipster Information

First Name: [REDACTED]

Middle Name:

Last Name: [REDACTED]

Phone: [REDACTED]

Email: [REDACTED]

Address: 13423 W 92nd St

City: Lenexa

State: Kansas

Zip: 66215

Country: United States

b6
b7C
b7E

[REDACTED]

Database Queries:

[REDACTED]

[REDACTED]

b7E

UNCLASSIFIED//~~FOUO~~

[REDACTED]
UNCLASSIFIED//~~FOUO~~

Title: (U) PAL2017 [REDACTED] E-Tip: Extortion
Re: [REDACTED] 06/29/2017

[REDACTED]
b6
b7C
b7E

.....
Final [REDACTED] Finding:

b7E

Open source research of this report from SMALL BUSINESS BANK indicates a sizable number of enterprises have received a similar or identical threat email from the same address. A search of Sentinel located a report made on the same day from a small business in Illinois with an identically worded email asking for Bitcoin using the same wallet address.

Internet security company Cloudflare published an article documenting hundreds of attempted scams using a similar email and found not one sustained an actual attack. It would not be possible for the sender to know which victim was paying since the same Bitcoin address, amount and time frame was used for multiple victims.

[REDACTED] of NETWORK TECHNOLOGIES was contacted by telephone at [REDACTED]. [REDACTED] NETWORK TECHNOLOGIES performs IT services for their client, SMALL BUSINESS BANK. [REDACTED] confirmed that SMALL BUSINESS BANK did not sustain any legitimate attack.

b6
b7C
b7E

Recommended Action: [REDACTED]

Entities:

Lizard Squad (Main, Organization, U.S. Person? Unknown)
Communication Account
Type: Email

UNCLASSIFIED//~~FOUO~~

[REDACTED]

UNCLASSIFIED//~~FOUO~~

Title: (U) PAL2017 [REDACTED] E-Tip: Extortion
Re: [REDACTED] 06/29/2017

b3
b6
b7C
b7E

Account: [REDACTED]

Small Business Bank (Complainant, Organization, U.S. Person? Unknown)

Location

Country: United States

[REDACTED] (Complainant, Person, U.S. Person? Unknown)

b6
b7C

Name/Biographical Information

Name: [REDACTED]

Minor? No

Has Diplomatic Status? No

Communication Account 1

Type: Email

Account: [REDACTED]

Communication Account 2

Type: Telephone

Account: [REDACTED]

Communication Account 3

Type: Telephone

Account: [REDACTED]

♦♦

UNCLASSIFIED//~~FOUO~~